

## UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

**FILED**  
 NOV 01 2019  
 Mark C. McCart, Clerk  
 U.S. DISTRICT COURT

In the Matter of the Search of  
 An Apartment located at 1109 Sandpiper Drive,  
 Pryor OK; 2006 Ford Fusion, Cherokee Nation  
 Plate CB5193; Samsung Model Galaxy 7,  
 Phone Number 918-568-5737

Case No., 19-mj-231-JFS

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2251	Sexual Exploitation of Children

The application is based on these facts:

See Affidavit of Matthew Hewett, attached hereto.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Matthew Hewett FBI SA

Printed name and title

Sworn to before me and signed in my presence.

Date: 11-1-19

City and state: Tulsa, OK Tulsa, Oklahoma

  
\_\_\_\_\_  
*Judge's signature*

U.S. Magistrate  
\_\_\_\_\_  
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF:  
AN APARTMENT LOCATED AT 1109  
SANDPIPER DRIVE, PRYOR, OKLAHOMA;  
2006 FORD FUSION, CHEROKEE NATION  
PLATE NUMBER CB5 193; SAMSUNG  
MODEL GALAXY 7, PHONE NUMBER 918-  
568-5737

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Matthew Hewett, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1109 Sand Piper, Pryor, Oklahoma, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been so employed since September, 2006. I am currently assigned to the Tulsa Resident Agency of the Oklahoma City Division. As a Special Agent with the FBI, Affiant is charged to investigate violations of Federal law, to include Title 18 United States Code § 2251, Sexual Exploitation of Children.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Affiant interviewed Travis Lloyd James on October 31, 2019 and requested his consent to seize and search his phone. James allowed me a cursory review of his phone, but refused to allow a full search of his phone. James reported his phone number is 918-568-5737 and his phone is a Samsung Galaxy 7.

**PROBABLE CAUSE**

5. On October 31, 2019, Affiant was contacted by Cherokee Nation Marshal Service Investigator Vince Smith. Smith emailed a Mayes County Sheriff's Office report 19-1524 to Affiant. This report documented a juvenile female, C.K., told her friend, H.M., that her stepfather was abusing her sexually. Furthermore, C.K. reported her stepfather was recording her in the shower.

6. Mayes County Sheriff's Office Investigator Damon Brandt learned C.K. attended Lincoln Elementary School in Pryor, OK. Brandt contacted Pryor Police School Resource Officer Tommy Parker who advised C.K.'s mother is Tiffany Wolfe. Wolfe lives at 508 Cherokee Heights in Pryor, Oklahoma. Cherokee Heights is Cherokee Tribal land, therefore, Investigator Brandt emailed a copy of report 19-1524 to Investigator Smith.

7. Smith determined C.K.'s stepfather is Travis Lloyd James, date of birth August 25, 1989. James works at Homeland in Pryor, Oklahoma. Smith and Affiant contacted James at Homeland on October 31, 2019. During the interview James stated he lived at 1109 Sandpiper Drive, Pryor, Oklahoma. Records searches indicated he lived in apartment 32. Officers later

observed James' red Ford Fusion parked outside the apartment building located 1109 Sandpiper Drive. James denied sexually abusing C.K. or taking videos of her in the shower. James reported a few months ago he saw scratches on C.K.'s back when she was undressed and in the shower. The scratches ran length-wise down C.K.'s back and stopped near her waist. James attempted to take pictures of C.K.'s back. He advised he was going to send the pictures to Wolfe who was at work. James reported he took one picture but C.K. told James not to take a picture and tried to cover herself. James never sent the picture to Wolfe who returned to James's apartment approximately two hours later. James allowed Affiant to look at some pictures on his Samsung 7 phone, but refused to turn his phone over for a consensual search. James continued to deny touching C.K. inappropriately or taking inappropriate pictures of C.K. James provided his Google account is [bestdaddyever89@gmail.com](mailto:bestdaddyever89@gmail.com). Affiant and Smith terminated the interview with James and left Homeland.

8. Affiant and Smith contacted Tiffany Wolfe at her residence in Cherokee Heights and advised her of the allegations regarding Travis James. Wolfe reported she and James met and began dating in 2012. She advised James had sexual addictions which involved pornography and receiving topless photos from other women while she and James were dating. Wolfe stopped reviewing James's phone around 2014 because she "always found something" such as deleted messages and porn sites. Wolfe never saw anything related to child pornography on James's phone.

9. During the summer of 2019, Wolfe saw a picture of C.K. on James's phone. When Wolfe tried to open the picture it was deleted. Wolfe noted the picture showed C.K.'s leg and "her region." Wolfe observed C.K. was laying in the tub/shower at James's apartment. She confronted James with the picture asking "what the fuck" is this? James explained C.K. had a bug bite on her leg and he was trying to take a picture of it to show Wolfe.

10. Soon after this, Wolfe broke up with James. Wolfe has noticed C.K. has been more withdrawn in the last few months. She reported James asks her why C.K. won't hug him anymore. Wolfe and James have a six year old son together and continue to interact occasionally. James has a daughter from a previous relationship. Prior to the summer of 2019, C.K. wanted to spend the night at James's apartment with his daughter. Wolfe observed C.K. no longer wants to stay at James's apartment, but will ask for James's daughter to stay at Wolfe's house.

11. Wolfe believes James has had approximately four cell phones since they began dating in 2012. James borrowed a small purple laptop from his mother a few months ago. Wolfe thinks he borrowed it so the kids could play games. She believes James still has this laptop.

12. Wolfe noted she and James would take turns watching each other's children while they were dating. James watched her children when she was at work and she watched his children when he was working. They would keep the children at either of their residences. However, recently Wolfe asked James to stay at her house because C.K. wanted to be at her home. Wolfe noted James stayed with the children a few times at her house.

13. Based on C.K.'s allegations James was recording her in the shower, James's admission he took a picture of C.K. in the shower and Wolfe observing a different picture of C.K. in the shower on James's phone, your Affiant requests a search warrant be issued to seize and search James's Samsung Galaxy 7 phone and the borrowed small purple laptop. Furthermore, because digital files can be easily transferred from one phone to another phone, laptop computer or other digital media, your Affiant requests authority to seize all phones, computers and digital media located on James's person, at his residence or in his vehicle.

14. On November 1, 2019, at approximately 11:50 AM, a red 2006 Ford Fusion with Cherokee Nation Plates Number CB5 193 was parked outside of the home. The vehicle is registered to Deborah James of 42 Lakeside Terrace, Rd. 1, Salina, Oklahoma. On October 31, 2019, Travis Lloyd James informed the affiant that he had purchased the car from his mother, Deborah, but had not changed the registration yet.

### **TECHNICAL TERMS**

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP

address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

16. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage



media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

17. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the

computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

19. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who

has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.


- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**CONCLUSION**

21. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

  
\_\_\_\_\_  
Matthew Hewett  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on November 1, 2019:

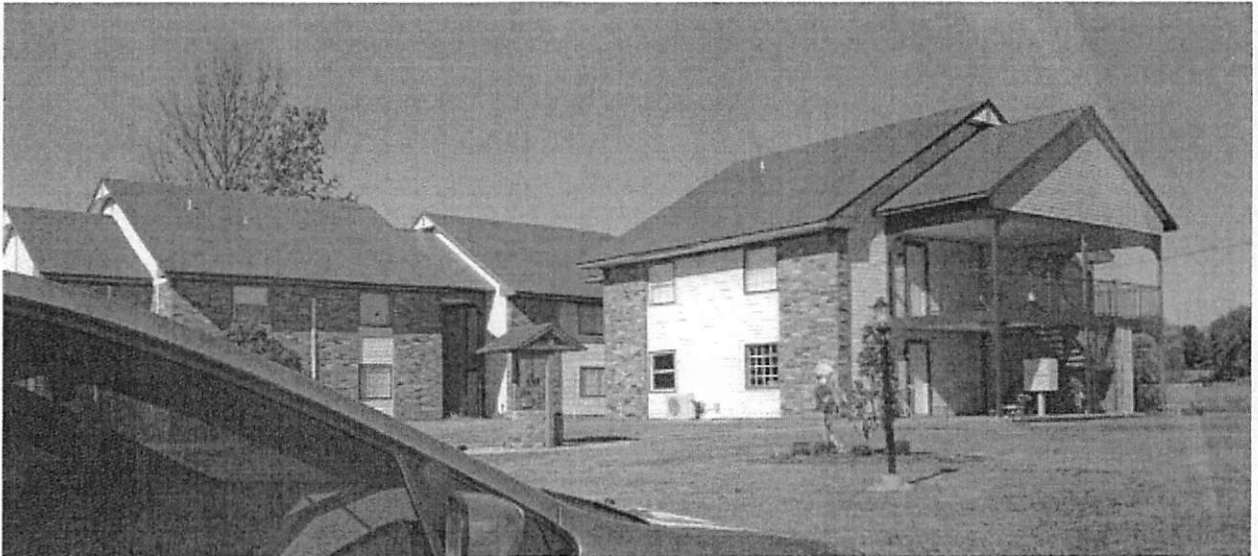
  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

*Property to be searched*

The property to be searched is 1109 Sandpiper Drive, Apartment 32, Pryor, Oklahoma, further described as a tan multifamily dwelling with balconies and stone facades:



A red 2006 Ford Fusion with Cherokee Nation Plates Number CB5 193:



The residence and vehicle shall be searched only while Travis Lloyd James is occupying the dwelling and/or vehicle or is otherwise in the vicinity of the property to be searched. Once the Samsung Galaxy 7 cellular telephone with phone number 918-568-5737 described in attachment B is seized, no other property may be searched pursuant to this warrant.

**ATTACHMENT B**

*Property to be seized*

1. All records relating to violations of 18 USC § 2251, those violations involving Travis Lloyd James and occurring after January 1, 2019, including:
  - a. Samsung Galaxy 7 cellular telephone with phone number 918-568-5737;